Towards a spectral approach for the design of self-synchronizing stream-ciphers

Jeremy Parriaux, Philippe Guillot, Gilles Millérioux

Towards a Spectral Approach for the Design of Self-Synchronizing Stream-Ciphers

Jérémy Parriaux[1], Philippe Guillot[2], and Gilles Millérioux[1]

[1] Nancy University, CNRS,
Research Center for Automatic Control of Nancy (CRAN UMR 7039), France,
jeremy.parriaux@esstin.uhp-nancy.fr, gilles.millerioux@esstin.uhp-nancy.fr,
[2] Université Paris 8
Laboratoire Analyse, Géométrie et Applications (LAGA UMR 7539), France
philippe.guillot@univ-paris8.fr

Abstract. This paper addresses the problem of self-synchronization of a class of dynamical systems involving Boolean functions. We motivate the work in the context of cryptography with the perspective of designing self-synchronizing stream ciphers and assessing their efficiency in terms of security. The self-synchronization is tackled through the notion of influence of variables. We propose a spectral characterization of the self-synchronization property through the Walsh transform. We discuss two kinds of self-synchronization: the finite time one and the statistical one.

1 Introduction

Stream-ciphers are cryptosystems well suited when the data to be encrypted are generated sequentially or when the encryption speed is a concern. Indeed, their simple structure usually allows higher throughput than block ciphers. Unlike block ciphers, they involve a time varying transformation applied to the plain-text giving rise to the interesting property that two identical plaintexts may have different ciphertexts. An important requirement for proper decryption is to guarantee that the decipher is well synchronized with the cipher. This is often ensured by resorting to synchronization protocols which introduce overheads in the stream conveyed through the channel. Such an approach applies for the so-called synchronous stream ciphers. A special class of stream-ciphers has the interesting property of self-synchronization. By self-synchronization, it is meant an intrinsic (also called structural) synchronization between the decipher and the cipher rendering the synchronization protocols useless. They are called self-synchronizing stream-ciphers (SSSC for short). And yet, it must be stressed that few attention has been paid on them. The reader may refer to [1] for details about the design of SSSC.

In this paper, we focus on the self-synchronization property for systems involving Boolean functions [2, 3] having in mind the cryptographic context and more specifically the use of self-synchronizing stream ciphers. The self-synchronization is tackled through the notion of influence of variables which is developed herein. Then, we propose a spectral characterization of the self-synchronization property. The layout is the following: Section 2 is devoted to the problem statement. Canonical equations of SSSC are recalled. In Section 3, we expose the main results which essentially consist in a spectral characterization of the self-synchronization property and the notion of influence of variables.

2 Problem Statement

Concealment in stream-ciphers is usually done by performing the exclusive-OR (denoted by $\oplus$) between the successive plaintext bits (denoted by p_t) and the bits of a key-stream (denoted by K_t). The index t stands for the discrete-time. The cipher and the decipher can be respectively modeled as dynamical systems governed by the sets of equations (1) and (2).

$$\begin{cases} x_{t+1} = f(c_t, x_t) \\ K_t \quad = g(c_{t-1}, x_t) \\ c_t \quad = K_t \oplus p_t \end{cases} \qquad \text{(cipher equation)} \tag{1}$$

$$\begin{cases} \widehat{x}_{t+1} = f(c_t, \widehat{x}_t) \\ \widehat{K}_t \quad = g(c_{t-1}, \widehat{x}_t) \\ \widehat{p}_t \quad = \widehat{K}_t \oplus c_t \end{cases} \qquad \text{(decipher equation)} \tag{2}$$

Let us call a (n,m)–function a function from the vector space $\mathbb{F}_2^n$ to the vector space $\mathbb{F}_2^m$. The vectors x_t and $\widehat{x}_t$ are respectively the state vectors of the cipher and of the decipher. The next-state function f is an $(n+1,n)$ function depending on the internal state x_t and on the cipher-text c_t. The $(n,1)$–function g delivers the key-streams K_t and $\widehat{K}_t$. Finally, $\widehat{p}_t$ stands for the recovered plain-text. For a proper decryption of the cryptogram c_t, the states x_t and $\widehat{x}_t$ must coincide at each discrete-time t. Roughly speaking, the compound system (1)–(2) is self-synchronizing if the coincidence $x_k = \widehat{x}_k$ is achieved whatever are the initial states x_0 and $\widehat{x}_0$, possibly after a transient time. In this sense, the synchronization is an intrinsic (or structural) property of the system. It can easily be seen that this property depends exclusively on the function f. Now, let us formally define the self-synchronization property. We denote by (c) the sequence $(c_0, \ldots, c_i)$.

Definition 1 (Self-synchronizing sequence). *A sequence (c) is self-synchronizing for f if there exists an integer t_c so that for all initial states x_0 and $\widehat{x}_0$*

$$\forall t \geq t_c,\ x_t = \widehat{x}_t \tag{3}$$

Definition 2 (Finite time self-synchronization). *The system (1)–(2) is finite time self-synchronizing if the minimum value t_c is upper bounded for all possible sequences (c). The upper bound t_c is called the self-synchronization delay of f.*

Remark 1. If (c) is a random sequence, then t_c is a random variable. In such a case, it should be denoted T_c.

Definition 3 (Statistical self-synchronization). *The system (1)–(2) is statistically self-synchronizing if $\lim_{t\to+\infty} \mathrm{Prob}(T_c \leq t) = 1$. T_c is called the random synchronization delay for the random sequence (c).*

3 Main Results

This section aims at establishing a spectral characterization of the self-synchronizing property through the Walsh transform. Such a property is expressed in terms of influence of variables which is developed.

3.1 Self-Synchronization and Influence

The function f involved in (1)–(2) is considered as a mapping $f(c,x) : \mathbb{F}_2 \times \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$. We define, for any positive integer t, the $(n+t+1,n)$–function ϕ_t which is the iterated function of f. It expresses the internal state after $t+1$ iterations and thereby depends on the initial internal state and the cipher-text sequence. For $x_0 \in \mathbb{F}_2^n$ and $(c) = (c_0,\ldots,c_t) \in \mathbb{F}_2^{t+1}$, $\phi_t(c,x)$ is defined as:

$$\phi_t(c,x) = f(c_t, f(c_{t-1}, f(\ldots, f(c_0,x_0)\cdots))) \tag{4}$$

The self-synchronization property can be directly related to the notion of influence. Indeed, it is worth pointing out that (1)–(2) has the self-synchronization property if there exists an integer t so that ϕ_t does not depend on x_0 anymore.
Therefore, the following proposition holds:

Proposition 1. *The system* (1)–(2) *is self-synchronizing if and only if x_0 has no influence over ϕ_t.*

The function ϕ_t playing a central role and having in mind a spectral characterization of the influence, we must state some properties of the corresponding Walsh transform.
Let us denote by f^0 (respectively f^1) the (n,n)–function which is the restriction of f to the input $c = 0$ (respectively to $c = 1$). For a given fixed input sequence (c), we denote by ϕ_t^c the (n,n)–function that expresses the internal state after $t+1$ iterations: $\phi_t^c : x \longmapsto \phi_t(c,x)$. The spectrum of the function ϕ_t restricted to the input sequence (c) is the Walsh matrix $W_{\phi_t^c}$ of ϕ_t^c.

Proposition 2. *The Walsh matrix of ϕ_t^c is*

$$W_{\phi_t^c} = \frac{1}{2^{n\cdot t}} W_{f^{c_t}} W_{f^{c_{t-1}}} \times \cdots \times W_{f^{c_0}}. \tag{5}$$

The spectrum of ϕ_t can be expressed in terms of the spectrum of f. For two vectors $u = (u_0,\ldots,u_t)$ and $v = (v_0,\ldots,v_{n-1})$, their concatenation, denoted $u|v$ is by definition the $(n+t+1)$–dimensional vector $u|v = (u_0,\ldots,u_t,v_0,\ldots,v_{n-1})$. We define the operator τ which transforms a binary vector $z = (z_0,\ldots,z_l)$ to the integer $\tau(z) = \sum_{t=0}^{l} 2^{l-t} z_t$.

Proposition 3. *The entry of the $2^n \times 2^{n+t+1}$ dimensional Walsh matrix of the iterated function ϕ_t is*

$$w^{\phi_t}_{s,\tau(u|v)} = \sum_{c\in\mathbb{F}_2^{t+1}} (-1)^{u\cdot c} w^{\phi_t^c}_{s,v} \tag{6}$$

3.2 Spectral Characterization of the Influence

Throughout the literature, see in particular [4, 5], the influence of a set S of variables over a function is often defined as the probability that there exists at least one way to change the value of the function by changing the value of the variables in the set, the variables not in the set being chosen at random. The fact that this definition has no usable spectral expression is a major drawback. And also, it does not take into account the number of possibilities of choosing the variables for changing the value of the function. We therefore rather introduce another definition of the influence that takes this point into account.

Definition 4. *The influence on a function f of a set S of variables is the mean of the probabilities that $f(x)$ changes when x is randomly chosen, the mean being computed for all possible changes of variables not in the set S.*

Recall that the support of a vector $u \in \mathbb{F}_2^n$ is by definition $\mathrm{supp}(u) = \{t \in \{1,\ldots,n\} \,|\, u_t \neq 0\}$.

Definition 5. *Let f be a $(n,1)$–function of a vector $x \in \mathbb{F}_2^n$ and S a set of ℓ components of x. The influence $I_f(S)$ is:*

$$I_f(S) = \frac{1}{2^n(2^\ell - 1)} \sum_{x\in\mathbb{F}_2^n} \sum_{u\in\mathbb{F}_2^n / u\neq 0,\ \mathrm{supp}(u)\subset S} [f(x) \oplus f(x \oplus u)] \tag{7}$$

It can be shown that $I_f(S)$ can be expressed by means of $\widehat{f_\chi}$ which is the Walsh transform of f. Notice that the correspondence between $\widehat{f_\chi}$ and the Walsh matrix fulfills $w_{1,\tau(v)} = \widehat{f_\chi}(v)$.

Proposition 4. *Let f be a $(n,1)$–function of a vector $x \in \mathbb{F}_2^n$ and S a set of ℓ components of x,*

$$I_f(S) = \frac{2^{\ell-1}}{2^{2n}(2^\ell - 1)} \sum_{v\in\mathbb{F}_2^n /\ \mathrm{supp}(v)\cap S\neq\emptyset} \widehat{f_\chi}^2(v) \tag{8}$$

We extend Definition 5 to a vectorial Boolean function that is to a (n,m)–function with $m \geq 1$.

Definition 6. *The influence of a set of variables S over a vectorial Boolean function $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^m$ is*

$$I_f(S) = \frac{1}{m} \sum_{j=1}^{m} I_{f_j}(S) \tag{9}$$

where f_j is the j^{th} coordinate function of f.

3.3 Spectral Characterization of the Self-Synchronization Property

In this section, we characterize the self-synchronization property based of the results stated above.

Finite Time Self-Synchronization We recall that the self-synchronization property is related to the existence of an integer t so that $\phi_t(c, x_0)$ does not depend on x_0 or equivalently to the fact that the initial state x_0 has no influence over ϕ_t. By virtue of (8) and (9), the influence is proportional to the sum of some squared Walsh coefficients. This yields the following proposition.

Proposition 5. *Let S_{x_0} be the set of n components of x_0 the initial state of the functions ϕ_t. The system (1)–(2) is finite time self-synchronizing if and only if there exists a corresponding iterated function ϕ_t so that,*

$$\forall v \in \mathbb{F}_2^n,\ \mathrm{supp}(v) \cap S_{x_0} \neq \emptyset,\ \forall j \in [0, 2^{n-1} - 1],\ \ w^{\phi_t}_{j,\tau(v)} = 0 \tag{10}$$

Statistical Self-Synchronization We now consider the case of the statistical self-synchronization property. If a system is statistically self-synchronizing, there exists at least one self-synchronizing sequence. It is possible to characterize such a sequence using the following proposition.

Proposition 6. *The sequence* (c) *of length* $t+1$ *is a self-synchronizing sequence if and only if the Walsh matrix of the function* ϕ_t^c *is of the form*

$$W_{\phi_t^c} = \begin{pmatrix} 2^n & 0 & \cdots & 0 \\ \pm 2^n & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ \pm 2^n & 0 & \cdots & 0 \end{pmatrix} \tag{11}$$

4 Concluding Remarks

We have focus on the self-synchronization property for systems involving Boolean functions. It is motivated by the fact that such a property is central when addressing cryptographic applications involving the special class of stream ciphers, namely the self-synchronizing ones. We expect that this work constitutes a first step towards a systematic methodology for the design of such ciphers. Indeed, the design amounts to finding suitable Boolean functions f so that the iterated function fulfills the spectral conditions provided in this note.

References

1. G. Millérioux and P. Guillot. Self-synchronizing stream ciphers and dynamical systems: state of the art and open issues. *International Journal of Bifurcation and Chaos, 20(9)*, 2010.
2. C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Boolean Functions for Cryptography and Error-Correcting Codes. In [6], 2010.
3. C. Carlet. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*, chapter Vectorial Boolean Functions for Cryptography. In [6], 2010.
4. J. Kahn, G. Kalai, and N. Linial. The influence of variables on boolean functions. In *SFCS '88: Proceedings of the 29th Annual Symposium on Foundations of Computer Science*, pages 68–80, Washington, DC, USA, 1988. IEEE Computer Society.
5. Nathan Keller. On the influence of variables on boolean functions in product spaces, May 2009. Availaible at: `http://arxiv.org/PS_cache/arxiv/pdf/0905/0905.4216v1.pdf`.
6. Y. Crama. *Boolean Models and Methods in Mathematics, Computer Science, and Engineering*. Cambridge Press, 2010.